



大会 — 第42届会议

执行委员会

议程项目 13: 航空安保 — 政策

国际民航网络安全的现行做法与改进

(由萨尔瓦多代表中美洲空中航行服务公司 (COCESNA)²成员国提交)

执行摘要

技术在航空领域发挥着至关重要的作用，它促进了旅游、贸易和全球互联互通，推动了经济增长并改善了生活质量。航空电子设备的进步已显著改善了导航管理、飞机安全和运营效率。这个领域的技术创新对于保持竞争力和满足日益增长的航空运输需求至关重要。

民航网络安全已成为保障安全和空中航行效率的基石。目前，航空业面临着动态的环境和不断演变的网络威胁，需要采取战略性的协调一致方法来保护关键基础设施。

本工作文件分析了航空领域当前采用的网络安全做法，提出了改进和未来实施中需要考虑的关键方面，以增强航空系统应对新出现的网络威胁的韧性。

行动：请大会：

- 表示注意到提供的信息；
- 请国际民航组织评估并加强网络安全战略，采取基于国际最佳做法、信息交流和新技术的方法；和
- 请国际民航组织继续支持各国建立和实施网络安全监管框架，培训和加强工作人员在该领域的能力，并制定将网络安全纳入国家航空安全计划 (NASP) 的网络韧性计划。

战略目标：

每次飞行都安全和安保
不让任何国家掉队
航空运输经济发展确保实现经济繁荣和全民社会福祉

财务影响：

参考文件：

国家标准和技术研究院 (NIST) 的监管框架
Doc 9985 号文件：《空中交通管理安保手册》
Doc 10075 号文件：《大会有效决议》(截至 2016 年 10 月 6 日)
Doc 10161 号文件：《全球航空安全路线图》
附件 17 — 《航空安保》

¹ 西班牙文文本由萨尔瓦多提供。

² 伯利兹、哥斯达黎加、萨尔瓦多、危地马拉、洪都拉斯和尼加拉瓜。

1. 引言

1.1. 技术在航空领域发挥着至关重要的作用，而技术进步为提供空中航行服务带来了巨大效益。基于性能的导航（PBN）、广播式自动相关监视（ADS-B）和空中交通管理（ATM）等各种系统改变了航班管理方式，提高了准确性、安全性和效率。这些系统优化了航线规划、减少了航班延误并妥善地使用了空域。

1.2. 随着民航运营越来越依赖互联互通的数字系统，而这些系统内的技术资源对于民航的安全高效运营至关重要，因此民航网络安全已变得不可忽视之事。技术发展带来了重大挑战，包括针对空中交通管制系统、机场和航空运营人的网络攻击。因此，保护这些系统免受网络威胁具有重要战略意义。必须维护这些系统的完整性和可用性，不遭受可能影响运营安全和航空运输连续性的中断。在此背景下，网络安全不仅可以保护数据和系统，还可以增强对全球空中航行基础设施的信任。

1.3. 为应对此类威胁，各国已根据国际民航组织、国际航空运输协会和欧洲航空安全局制定的国际标准实施了各种网络安全措施。然而，目前仍存在一些差距需要弥补，以确保航空生态系统得到全面保护。

1.4. 本文件以三份国际民航组织大会决议为基础：A39-19 号决议 — 表明国际社会认识到网络安全是民航的当务之急；A40-10 号决议 — 提出合作和多学科方法；A41-19 号决议 — 重申解决网络安全和网络韧性的紧迫性。

2. 中美洲空中航行服务公司（COCESNA）当前实施的网络安全做法

2.1 实施国际民航组织（ICAO）网络安全框架的重要性已被充分考虑，该框架旨在识别、防御、检测、响应和恢复网络事件。目前正在与国际航空运输协会（IATA）、欧洲空中航行安全组织（EUROCONTROL）和欧洲航空安全局（EASA）等国际组织协调，在地区内外分享最佳实践。

2.2 在网络风险管理方面，COCESNA 正在为应用风险分析方法（ISO 27001、NIST 和 MITRE ATT&CK）奠定基础。这些方法的实施有助于持续评估航空系统的脆弱性，并将网络安全纳入中美洲地区的空中航行服务系统。同样，COCESNA 打算建立一个安保运营中心（SOC），以便通过持续监控、高级威胁分析和快速事件响应加强其处理安保事件的能力。通过这项服务，我们力求实施一种战略性的高效方法来保护系统、数据和用户，最大限度地降低风险，并确保业务连续性和法规合规性。

2.3 在培训和提高意识方面，我们目前正在为所有公司人员制定网络安全基础培训，并将开设专门课程，为特定人员提供网络安全最佳做法和趋势的培训。

3. 改进航空网络安全需要考虑的方面

3.1 可以通过创建安全的平台来实时共享威胁和漏洞信息，从而与其他空中航行服务提供者建立合作和信息交换。这可通过多边协议来加强地区网络安全合作的方式来实现。

3.2 应制定并实施一个规范网络安全的监管框架。这样的框架应提供明确的准则和标准，供各机构遵循，以保护其数字资产和维护其数据机密性。实施强有力的监管框架将有助于降低风险、预防安保事件发生并确保运营连续性。

3.3 网络安全培训计划应涵盖技术和实践方面，例如事件管理、风险分析和保护措施的实施。此外，培养沟通和协作技能也至关重要，这样工作人员才能成为协作无间的团队，共享网络安全知识。对培训作出投资是符合经济效益的战略，它增强了机构应对网络威胁的能力。

3.4 加强工作人员之间的网络安全意识有助于减少人为错误，而人为错误是导致网络安全事件的主要原因。根据世界经济论坛《2022 年全球风险报告》等研究，95%的网络安全问题都是由人为错误造成的。威胁意识和网络安全最佳做法有助于营造以数字安全为中心的机构文化。

3.5 我们应制定网络韧性计划，将网络安全纳入国家航空安全计划（NASP）。该计划需要纳入网络攻击复原战略，以便最大限度地减少对运营产生影响。

3.6 我们必须积极主动地识别和解决漏洞，以保护技术基础设施并确保数据安全。

3.7 与来自科技、银行和其他领域等不同行业的网络安全专家合作，可以带来宝贵的知识和专业资源，从而增强对航空系统的保护。

3.8 人工智能和云计算等新出现的技术的采用为提高民航的效率和安全性提供了机遇。然而，至关重要是，这些技术的实施必须采取强有力的网络安全措施，以防范可能存在的漏洞和威胁。这些技术的安全整合可能会改变整个行业，但需要周密的规划和适当的风险管理。

4. 结论

4.1 网络安全是民航运行安全和效率的关键要素。保护航空系统免受网络威胁对于确保运行安全和航空运输的连续性至关重要。虽然在实施保护措施方面已取得重大进展，但仍存在需要立即关注的挑战。

4.2 通过安全平台和多边协议加强航空领域各机构之间的国际合作和信息交流对于提高网络安全至关重要，同时，整合先进技术并采取积极主动的方法进行国际民航网络风险管理。

4.3 ISO/IEC27001 和 NIST CSF 等国际标准的实施将为保护数字资产和确保数据机密性提供明确的指导方针，有助于降低风险并预防事故。

4.4 培训工作人员并提高网络安全意识可以减少人为错误、加强威胁响应能力并增强机构韧性。

4.5 为了保护技术基础设施，必须通过风险评估、升级、渗透测试和持续监控来主动识别和解决漏洞。

4.6 与各行业网络安全专家合作，并与安保运营中心（SOC）和 MSSP 等专门服务公司签订合同，可以实现持续监控和快速事件响应，确保更好地保护航空系统。

4.7 将人工智能和云计算等技术与强大的网络安全措施相结合，为提高民航安全和效率及确保安全有效地采用这些技术提供了机会。